(2)

WEAPON SYSTEM EXPLOSIVES SAFETY REVIEW BOARD

TECHNICAL MANUAL FOR ELECTRONIC SAFETY AND ARMING DEVICES WITH NON-INTERRUPTED EXPLOSIVE TRAINS

30 Sept 1990

WSESRB Technical Manual for Electronic Safety and Arming Devices with Non-Interrupted Explosive Trains

Forward

1. Munition fuzes historically have utilized sensitive explosive elements whose output has been physically interrupted until arming. Control of the arming process in these fuzes was accomplished by mechanical means. The advent and rapid advancement in solid state electronics has furnished alternatives for fuze safety design. In recent years, advances in explosive initiation elements have provided an option for eliminating the need for physical interruption of the explosive train. The application of these technological advances is addressed in this manual.

2. This Technical Manual is for use in the design of fuzes and other initiating systems to be used by the United States Navy as a supplement to the requirements of MIL-STD-1316.

3. Beneficial comments (recommendations, additions, deletions) and any pertinent data which may be of use in improving this document shall be addressed to:

Chairman
Weapon System Explosives Safety Review Board
Naval Sea Systems Command
Washington, DC 20362.

Comments should be forwarded through the appropriate Systems Command for each project.

4. This manual extends specific design safety criteria for fuzes and other initiating systems beyond that covered by MIL-STD-1316 and specifically applies to the safe and arm functions used in weapon systems which have in-line explosive or initiator trains. This manual provides additional design criteria for fuzes and safety and arming devices (with non-interrupted explosive trains) that do not fully meet the requirements of MIL-STD-1316C. Although it repeats some information from MIL-STD-1316, it does not supersede these requirements for systems that comply with the requirement for non-interrupted explosive trains with two physical locks.

5. The safe and arm requirements specified herein are mandatory fundamental elements of design, engineering, production, and procurement. Fuzes and initiating systems shall provide safety that is consistent with mission requirements throughout the assembly, handling, storage, transportation, use, and disposal phases of the system life cycle.

WSESRB Technical Manual for
Electronic Safety and Arming Devices
with Non-Interrupted Explosive Trains

Table of Contents

WSESRB Technical Manual for Electronic Safety and Arming Devices with Non-Interrupted Explosive Trains

1. SCOPE

1.1 Purpose

MIL-STD-1316 establishes design safety criteria for fuzes and Safety and Arming (S&A) devices that are subsystems of fuzes. This document supplements MIL-STD-1316 by providing additional safety design criteria for electronically controlled fuzes, S&As, and initiation systems. Hereinafter, these fuzes and S&As are referred to as Electronic Safety and Arming Devices (ESADs).

1.2 Scope of Applicability

This document applies to the design of ESADs having electronic or partly electronic means of arming and firing and not having interrupted explosive trains. It applies to all ordnance used or transported by the Navy. Within the scope of this document, ESADs include items commonly referred to as fuzes, safety and arming devices (S&As or SADs), arm fire devices (AFDs), ignitions safety devices (ISDs), etc. This document applies to the design of electronic Arm-Fire Devices (AFDs), hand emplaced ordnance, and other items to the extent specified in the Appendices.

1.3 Excluded munitions

This standard does not apply to fuzes and S&A devices for Nuclear warheads.

2. APPLICABLE DOCUMENTS

2.1 Government Documents

2.1.1 Specifications, Standards and Handbooks

The following specifications, standards, and handbooks form a part of this document to the extent specified herein. Unless otherwise specified, the issues of these documents are those listed in the issue of the Department of Defense Index of Specifications and Standards (DODISS) and supplement thereto, cited in the solicitation (see 6.2).

FEDERAL SPECIFICATIONS

MIL-I-23659	Initiators, Electric, Design and Evaluation of

MILITARY STANDARDS

MIL-STD-331	Fuze and Fuze Components, Environmental and Performance Tests for
MIL-STD-444	Nomenclature and Definition in the Ammunition Area
MIL-STD-461	Electromagnetic Interference Characteristics, Requirements for
MIL-STD-882	System Safety Program Requirements
MIL-STD-1316	Fuze System Safety Design Criteria
MIL-STD-1385	Preclusion of Ordnance Hazards in Electromagnetic Fields, General Requirements for
DOD-STD-1463	Evaluation of Munitions to Electromagnetic Fields, Requirements for
MIL-STD-1512	Electro-Explosive Subsystems, Electrically Initiated, Design Requirements and Test Methods
MIL-STD-1757	Lightning Qualification Test Techniques for Aerospace Vehicles and Hardware
DOD-STD-1795	Lightning Protection of Aerospace Vehicles and Hardware
MIL-STD-1902	Explosive Ordnance Disposal, Munition Design Requirements for (Draft)
DOD-STD-2167	Software Development Standards for Military Systems
DOD-STD-2169	High Altitude Electromagnetic Pulse (HEMP) Environment

(Unless otherwise indicated, copies of federal and military specifications, standards and handbooks are available from the Naval Publications and Forms Center, (ATTN: NPODS), 5801 Tabor Avenue, Philadelphia, PA 19120-5099.)

2.1.2 Other Government Documents, Drawings and Publications

The following other Government documents, drawings and publications form a part of this document to the extent specified herein. Unless otherwise specified, the issues are those cited in the solicitation.

OTHER PUBLICATIONS

AFSC DH 1-6	Design Handbook, System Safety
NAVORD OD44811	Explosive Qualification Criteria
NAVORD OD44942	Weapon System Safety Guidelines Handbook
NAVSEAINST 8020.5B	Technical Requirements for Insensitive Munitions
NAVSEANOTE 9310	Responsibilities and Procedures for the Naval Lithium Battery Safety Program
ADA-086259	Joint Services Safety and Performance Manual for Qualification of Explosives for Military Use
NUREG-0492	Fault Tree Analysis

3. DEFINITIONS

3.1 General

The definitions of MIL-STD-444 generally apply to the munition terms in this standard and the definitions of ADA-086259 apply to the explosive terms. For interpretation of this standard, the following specific definitions apply:

3.1.1 Arm. To make a fuze or initiating system ready to function. ESADs are armed when they contain, or can result in the generation of, a stimulus that is greater the maximum allowable safe stimulus (MASS), and only a firing signal is required to deliver the stimulus to the initiator

3.1.2 Arm-Fire Devices (also Ignition Safety Devices). A device that prevents arming and functioning of a munition propulsion system until an acceptable set of conditions has been achieved.

3.1.3 Arming delay. The time elapsed, or distance traveled by the munition, from launch to arming (see 3.1.38).

3.1.4 Assembled fuze or initiating system. The completed fuze or initiating system with all component parts put together; a fuze or initiating system requiring no added components or parts to prepare it for installation into the munition in which it is to function. Assembling the fuze or initiating system is the process of putting the parts and components together.

3.1.5 Booster and lead explosives. Booster and lead explosives are compounds or formulations, such as those explosives listed in table I of MIL-STD-1316, which are used to transmit and augment the detonation reaction.

3.1.6 Credible environments. All environments that the system may encounter during its life cycle from initial manufacture to use or final disposal. Lightning strike and nuclear effects, including electromagnetic pulse and radiation, shall be considered credible environments for military systems.

3.1.7 Dud. A munition which has failed to function, although functioning was intended.

3.1.8 Dynamic electrical safety feature. An electrical design feature (energy interrupter) which continuously cycles between two or more states at a rate and in a pattern or results from a unique environment that will not be induced unintentionally during any credible life cycle phase and which, on its own or combined with another safety feature, provides a fail safe design.

3.1.9 Early-function. A fuze or initiating system function which occurs after the arming delay has been achieved but prior to valid target encounter or proper firing stimulus.

3.1.10 Electronic Safety and Arming Devices (ESADs). Safety and arming devices with non-interrupted explosive trains and use electrical function energy, including those that derive functioning energy from the post launch environment. ESADs include items commonly known as fuzes, safety and arming devices (S&As or SADs), arm fire devices (AFDs), ignitions safety devices (ISDs), etc.

3.1.11 Enabling. The act of removing or activating one or more safety features designed to prevent arming, thus permitting arming to occur subsequently.

3.1.12 Environment. A specific physical condition to which the fuze, S&A, or initiating system may be exposed.

3.1.13 Environmental stimulus. A specific stimulus obtained from an environment.

3.1.14 Explosive Ordnance Disposal. The detection, identification, field evaluation, rendering safe, recovery, evacuation and disposal of explosive ordnance which has been fired, dropped, launched, projected or placed in such a manner as to constitute a hazard to operations, installations, personnel, and materiel.

3.1.15 Explosive train. The detonation or deflagration train (i.e., transfer mechanism), beginning with the first explosive element (e.g., primer, detonator) and terminating in the main charge (e.g., munition functional mechanism, high explosive, pyrotechnic compound).

3.1.16 Fail-safe design. A characteristic of an ESAD or part thereof, designed to prevent munition function when components fail.

3.1.17 Firmware. The combination of a hardware device and computer instructions or computer data that reside as read-only software on the hardware device. The software cannot be readily modified under program control. Note that firmware is subject to the same development, analysis, and test requirements as software.

3.1.18 Function. The act of producing an output capable of initiating a train of fire or detonation in a munition.

3.1.19 Fuze or Initiating System. A physical system designed to sense or respond to one or more prescribed conditions, such as elapsed time, pressure, or command, and initiate a train of fire or detonation in a munition. Safety and arming are primary roles performed by a fuze or initiating system to preclude initiation of the munition before the desired position or time.

3.1.20 Fuze or initiating system installation. The act of installing or inserting the assembled fuze or initiating system into the munition in which it is to function.

3.1.21 Hand Grenades. Hand thrown ordnance items that are partially armed manually prior to throwing.

3.1.22 Handheld Ordnance Devices. Ordnance items that are launched or fired while held by ordnance personnel.

3.1.23 Independent safety feature. A safety feature is independent if its integrity is not affected by the function or malfunction of other safety features.

3.1.24 Initiator. A device capable of directly causing functioning of the explosive or pyrotechnic train in the fuze or initiating system.

3.1.25 Interrupted explosive train. An explosive train in which the explosive path between the primary explosives and the lead and booster (secondary) explosives is functionally separated until arming.

3.1.26 Launch cycle. The period between the time the munition is irreversibly committed to launch and the time it leaves the launcher.

3.1.27 Main charge. The explosive or pyrotechnic charge which is provided to accomplish the end result in the munition, e.g., producing blast and fragments, dispensing submunitions, or producing other effects for which it may be designed.

3.1.28 Manual arming feature. A design feature which can be activated by hand at any time and is not associated with a distinct sequence of events or time.

3.1.29 Manually Emplaced Ordnance Items. Explosive devices designed to be placed on their target manually.

3.1.30 Maximum Allowable Safe Stimulus (MASS). The greatest initiator stimulus which does not cause unsafe degradation or firing of more than one in one million initiators of a given design. Stimulus refers to the characteristics such as current, rate of change of current (di/dt), power, voltage, or energy, which is (are) most critical in defining the no-fire performance of the initiator.

3.1.31 Mechanical safety feature. Mechanical design feature which on its own or combined with another safety feature prevents unintentional arming or prevents functioning.

3.1.32 Neutralization. The process by which a munition is rendered, by external means, incapable of functioning on exposure to a target, although it may remain dangerous to handle.

3.1.33 Non-interrupted explosive train. An explosive train which provides interruption separating the elements in the explosive train.

3.1.34 Premature function. An ESAD function before completion of the arming delay.

3.1.35 Primary explosives. Primary explosives are sensitive materials, such as lead azide or lead styphnate, which are used to initiate detonation. They are used in primers or detonators, are sensitive to heat, impact or friction and undergo a rapid reaction upon initiation.

3.1.36 Pyrotechnic train. The burning or deflagration train beginning with the first pyrotechnic element (e.g. primer) and terminating in the main pyrotechnic compound.

3.1.37 Safe Condition. An ESAD is considered to be in a safe condition when less than the Maximum Allowable Safe Stimulus (MASS) has been accumulated and all safety features are in their safe state.

3.1.38 Safe separation distance. The minimum distance between the delivery system (or launcher) and the launched munition beyond which the hazards to the delivery system and its personnel resulting from the functioning of the munition have an acceptable level of risk as defined by the service safety authority. (See 4.2.2 and 4.2.2.3)

3.1.39 Safety and Arming Device. A device that prevents fuze or initiating system arming and functioning until an acceptable set of conditions has been achieved.

3.1.40 Safety feature. An element or combination of elements that prevents unintentional arming or functioning.

3.1.41 Safety Interlock. A design feature that prevents another design feature from activating or functioning thus preventing a safety system failure.

3.1.42 Safety system. The aggregate of devices (including hardware and software) included in the ESAD to provide safety and prevent arming and functioning until the prescribed arming and delay conditions have been achieved.

3.1.43 Safety system failure. A failure of the safety system to prevent unintentional arming or functioning.

3.1.44 Sensor, environmental. A component or series of components designed to detect and respond to a specific environment.

3.1.45 Sterilization. The act of permanently rendering a munition or ESAD inoperative beyond a predetermined time after laying or deployment.

4. GENERAL REQUIREMENTS

4.1 General

The following general requirements apply to all Electronic Safety and Arming Devices and their components within the scope of this document.

4.1.1 Compatibility of fuze or initiating system elements

Explosive compositions in fuzes and initiating systems shall be qualified in accordance with NAVORD OD 44811 and NAVSEAINST 8020.5B in their intended roles as explosive train components. All fuze or initiating system materials shall be chosen to be compatible and stable so that under all credible life-cycle conditions none of the following can occur in an unarmed fuze:

a. Premature arming
b. Dangerous ejection of material
c. Burning, deflagration, explosion, or detonation of the initiator, detonator, lead or booster
d. An increase in the sensitivity of explosive train components beyond the level at which they were approved for service use
e. Compromise of safety, sterilization, or explosive ordnance disposal features
f. Production of unacceptable levels of toxic or other hazardous materials or by-products

The compatibility of materials shall be verified by testing.

4.2 ESAD Safety Systems

The ESAD safety system design shall not contain any common mode or single point failures that could permit unintentional or early arming. The following general requirements apply to the design of safety systems. The ESAD design shall prohibit premature ESAD arming or functioning as a result of any or all of its electrical safety or energy control features failing in any given state. These failure modes include either random or induced failures which occur prior to, during, or after application of electrical power to the ESAD.

4.2.1 Safety redundancy.

ESAD safety systems shall contain at least two independent safety features, each of which shall prevent unintentional arming of the ESAD. The stimuli enabling the safety features (see Figure 1) shall be derived from different environments. Operation of at least one of these safety features shall depend on sensing an environment after first motion in the launch cycle or on sensing a post-launch environment. The effectiveness of each safety feature shall be determined by tests and analyses that account for all credible environments in the logistic cycle.

4.2.1.1 Enabling environments. Environments that enable safety features in ESADs shall not be conditions that pre-exist within the munition. Environments may be combined to enable electrical or mechanical

safety features, and a single environment may contribute to the enabling of more than one safety feature. No single environment shall be capable of enabling more than one safety feature. At least one sensed environment shall be verified continuously until munition safe separation is assured unless no practical environment is available. An action taken to initiate launch may be considered an environment if: the action is intentional and occurs only when launch is intended, and; the signal generated by the action irreversibly commits the munition to complete the launch cycle.

4.2.1.2 Dynamic electrical safety feature(s). The ESAD shall incorporate at least one safety feature (energy interrupter) which shall prevent unintentional arming when any combination of or all energy interrupters fail statically. This requires that at least one of the energy interrupters be electrically dynamic in its enabling functions during the arming process (see definition in 3.1.10). Improper operation or failure of the dynamic safety feature shall result in any arming energy being dissipated and shall prevent its accumulation above the safe condition (See section 3.1.37). The dynamic electrical energy interrupter shall be enabled by an environment after first motion in the launch sequence or on sensing a post launch environment. The environment must not be produced within the pre-launched weapon system or by the pre-launch environment. For systems that accumulate functioning energy from the post launch environment, see paragraph 5.2.4.1.

4.2.1.3 Launch environments. For warhead fuzes, operation of at least one of the independent features shall depend on sensing an environment after first motion in the launch cycle or on sensing a post-launch environment.

4.2.1.4 Physical partitioning. Electronic circuits controlling independent safety features shall be physically partitioned into functionally dissimilar elements, neither of which can independently arm the system. The functional partitioning shall ensure that the circuits are immune to common mode failures resulting from any credible environmental hazards. System arming shall not occur if any system electrical power sources, electrical grounds, or system frequencies are connected or disconnected in a credible manner to any point in the circuit.

4.2.1.5 Manual Arming Features. When a manual arming feature is used (see definition 3.1.28), such as a lanyard or umbilical disconnect, the design of the ESAD shall meet the system safety failure rate after this arming feature has been compromised (e.g., by removal of the lanyard) unless it can be shown by analysis and test that the feature will not be compromised by any credible life cycle environment.

4.2.1.6 Safety feature type combinations. Dynamic safety features provide greater safety than non-dynamic electrical safety features. Therefore, the number of required safety features in a system varies with the type. Figure 1 shows combinations are acceptable when supported by the appropriate safety analyses and test data. All safety features shall be independent (see 3.1.23). Combination option A represents compliance with MIL-STD-1316.

4.2.1.7 Safety Interlocks. The ESAD design shall incorporate at least one safety interlock that prevents completion of an abnormal arming sequence.

Safety Feature Type	Combination Options			
	A	B	C	D
Mechanical Safety feature	2	1	0	0
Dynamic Electrical Safety feature	0	1	2	1
Non-Dynamic Electrical Safety feature	0	0	0	2

Figure 1
Safety Feature Type Combinations
for Electronic Safety and Arming Devices

4.2.2 Arming delay

4.2.2.1 Safe Separation Safety. A safety feature of the ESAD shall provide a delay ensuring that a safe separation distance can be achieved for all anticipated operational conditions. Unacceptable rates of post-launch or post-deployment arming and functioning prior to safe separation shall be separately specified in the system requirements document or determined by the service safety authority.

4.2.2.2 Timers. When a timer or clock is used to provide an arming delay or control other safety critical functions, the ESAD shall be protected against failures in the clock or timer that can result in an early time-out. Redundant timers shall comply with paragraph 4.2.1.4 and shall be designed to preclude single-point and common mode failures from causing an early time-out.

4.2.2.3 Post-safe separation safety. When operational requirements necessitate protection of friendly forces in addition to the delivery system and its personnel, one of the following options shall be incorporated in the fuze or initiating system design:

a. Delay shall be extended to provide the required protection.
b. Unintentional functioning after proper arming delay, until attainment of the required protection, shall be controlled.

The design requirements document shall specify a minimum quantitative failure rate for the time frame after safe separation to the attainment of the required protection for the selected option.

4.2.3 Manual arming

An assembled system shall not be capable of being fully armed manually or inadvertently. Systems which employ manual arming features (see definition 3.1.28) shall meet the requirement of paragraph 4.2.1.5 of this document.

4.2.4 Logic functions

Any logic functions related to safety elements performed by the system shall be implemented in hardware or embedded in firmware.

4.2.5 Firmware

Firmware shall not be erasable or alterable by any credible environment encountered in the logistic cycle. For systems in which a fire control system or other system is required to preset data in firmware, the munition and fuze shall be designed such that they are incapable of altering or erasing the firmware data after loading. The munition shall be capable of performing reasonableness and sanity checks on the data loaded by the fire control system or other system.

4.2.6 Application Specific Integrated Circuits

4.2.6.1 ASIC Design

Application Specific Integrated Circuits (ASICs) shall comply the circuit design requirements of this document including sections 4.2.1.4, 4.2.4, 4.2.5, and other sections as applicable. ASICs shall not incorporate unnecessary gates or functions in the design. Power circuits should be isolated from signal or low power logic lines to the maximum extent practical through pin selection and circuit design. Multiple pin grounds are recommended to reduce ground inductance. High current transients (e.g., capacitor discharge) should not discharge through safety logic circuits.

4.2.6.2 ASIC Testing

ASICs used for safety critical circuits should be subjected to dynamic burn-in tests rather than static burn-in tests, i.e., the circuit should be required to operate during the burn-in test.

4.3 Safety system failure rate

The ESAD safety system failure rate shall be calculated by performing safety analyses and tests and shall be verified to the maximum extent practical by test and analysis during evaluation. As a minimum requirement, the safety system failure rate shall not exceed one failure in one million systems prior to intentional initiation of the arming sequence. For tube launched ammunition, this requirement extends to tube exit. Rates of post-launch arming and functioning prior to safe separation shall not exceed those specified in the system requirements document or as determined by the service safety authority.

4.3.1 Analyses

Analyses shall be performed to identify hazardous conditions for the purpose of their elimination or control. A Preliminary Hazard Analysis shall be conducted to identify the hazards of normal and abnormal environments, conditions and personnel actions that may occur in the phases before safe separation or disposal of the munition. This analy-

sis shall be used in the preparation of system design requirements. Hazard analyses, such as Failure Modes and Hazardous Effects Analyses (FMHEA), Failure Modes and Effects Criticality Analysis (FMECA), and Fault Tree Analyses (FTA), shall be conducted to arrive at an estimate of the safety system failure rate and to identify any potential single point failure or common mode failures. These analyses shall be reviewed by an independent establishment approved by the cognizant reviewing authority. For any systems using an embedded controller, micro-processor or other computing device, the analyses shall include a determination of the contribution of the embedded computing device, including its computer code to the enabling of the safety features. Where the computing device is shown to control or directly (critically) influence the removal of one or more safety features, a detailed safety analysis and safety testing of the computer code shall be performed to ensure that no design weaknesses, credible failures, or credible hardware failures propagating through the computer code, can result in compromise of the safety features. Techniques for conducting the FMHEA, FTA and other hazard analyses are described in NAVORD OD 44942, AFSC Design Handbook DH 1-6, NUREG-0492, and MIL-STD-882.

4.4 Design for quality control, inspection and maintenance

a. ESADs shall be designed and documented to facilitate application of effective quality control and inspection procedures. Design characteristics critical to the safety of the ESAD shall be identified to assure that the designed safety is maintained.
b. The design of the ESAD shall facilitate the use of inspection and test equipment for visual, physical, or electronic monitoring of all characteristics which assure the safety and intended functioning at all appropriate stages. The design should facilitate the use of automatic inspection equipment.
c. Embedded computing systems and their associated software (firmware) shall be designed and documented for ease of future maintenance. Software development shall be done in accordance with accepted high quality software development procedures, such as DOD-STD-2167A.

4.5 Design approval

At the inception of engineering development, the developing activity should obtain interim approval from the cognizant safety authority of both the design concept and the methodology for assuring compliance with safety requirements. At the completion of engineering development, the developing activity shall:

a. Exercise standing procedures in preparing for system safety reviews other than as noted in this document.
b. Prepare an ESAD System Safety Guideline Compliance Report documenting the compliance of the ESAD with the requirements imposed by this document. This report shall contain a detailed implementation description for each requirement.
c. Provide copies of the ESAD System Safety Guideline Compliance Report to the appropriate Systems Command offices who will

provide concurrence, comments and coordination of the waiver and safety approval in accordance with current directives.

4.6 Design features

4.6.1 Stored energy

The ESAD safety system shall not utilize stored energy to enable safety features or provide arming energy unless no adequate environmentally derived energy source is available. If stored energy is used, it shall be demonstrated that safety is not compromised and that the design complies with the requirements of 4.3 and 4.3.1. Examples of stored energy components are:

a. Batteries
b. Charged capacitors
c. Compressed gas
d. Explosive actuators (bellows and dimple motors, etc.)
e. Loaded springs

4.6.1.1 Lithium Batteries

Lithium batteries shall not be used in ESAD designs unless alternative battery designs are not available or not practical. Lithium batteries used in ESADs shall comply with the policy and requirements of NAVSEA Notice 9310. This requirement applies to ESADs for devices used aboard ships as well as those carried aboard ships in stowage.

4.6.2 Explosive ordnance disposal (EOD)

ESADs shall comply with the explosive ordnance disposal design requirements of MIL-STD-1902 (draft).

4.6.2.1 EOD Design Features. ESADs shall incorporate features that facilitate the neutralization of duds by EOD tools, equipment and procedures, if effective sterilization or self-destruction features are not incorporated. All ESADs shall have an EOD Render Safe Procedure and an EOD Disposal Procedure developed in accordance with MIL-STD-1902 (draft) during the development program.

4.6.2.2 EOD reviewing authority. All new or altered designs, or new applications of approved designs, shall be presented to the affected service's EOD Research, Development, Test and Evaluation authority for technical advice and assistance in determining viable design approaches or trade-offs for EOD and approval as follows:

a. For Army: Commander
US Army ARDEC
ATTN: SMCAR-FSM-E
Picatinny Arsenal, NJ 07806-5000

b. For Navy:
Commanding Officer
Naval Explosive Ordnance
Disposal Technology Center
ATTN: Fleet Liaison Office
Indian Head, MD 20640-5070

c. For Marine Corps:
Commanding Officer
Naval Explosive Ordnance
Disposal Technology Center
ATTN: Marine Corps Detachment
Indian Head, MD 20640-5070

d. For Air Force:
Commanding Officer
Naval Explosive Ordnance
Disposal Technology Center
ATTN: Detachment 63 US Air Force
Indian Head, MD 20640-5070

4.6.3 Safe condition

4.6.3.1 Safe condition assurance options. In order to allow the safe condition of an ESAD to be assured, designs shall incorporate one or more of the following features:

a. A feature(s) that prevent the assembly of the fuzing system in other than a safe condition.
b. A feature that provides a positive means of determining the safe condition of the system during and after assembly and when installing the system into a munition.
c. A feature that prevents the installation of an armed fuzing system into a munition.

If arming and reset of the assembled ESAD in tests is a normal procedure in manufacturing, inspection, or at any time prior to its installation into a munition, prevention of unsafe assembly (subparagraph a) is not sufficient and the provisions of either subparagraph b or c must also be met.

4.6.3.2 Visual indication. If visual indication of the safe-armed condition is to be employed in the ESAD, visible indicators shall be designed to provide a positive, unambiguous indication of the fuze or initiating system condition. The indicators shall be designed such that credible failures cannot result in a false 'safe' indication. If color coding is used to show the fuze or initiating system safe or armed condition, the colors shall be selected as follows:

a. Safe condition. Fluorescent green background with the letter S or word SAFE superimposed thereon in white. Colors shall be nonspecular.
b. Armed condition. Fluorescent red background with the letter A or the word ARMED superimposed thereon in black. Colors shall be nonspecular.

If other indicator capabilities are provided, they shall be designed to provide a positive indication of the safe or armed state of the ESAD and shall preclude the inadvertent input of any stimulus to the ESAD from the monitoring circuits.

4.6.4 Firing Stimulus Dissipation

The design of the firing circuit shall incorporate circuits or devices on the firing capacitor or other energy storage device to dissipate accumulated firing stimuli if functioning does not occur in a reasonable period of time. The discharge circuits or devices shall be designed to fail safe (i.e., to dissipate accumulated firing stimuli in the event of a failure) and to minimize the probability of common mode failures. The circuits shall be designed to reduce the accumulated firing stimuli to a level at or below the MASS within thirty (30) minutes of the time of expected function of the ESAD.

4.7 Electromagnetic and electrical hazards

The general requirements and test methods for the design and development of electro-explosive subsystems and associated items to preclude hazards from unintentional initiation are provided in MIL-STD-1512. Applicable portions of this standard and those specified in 4.7.1, 4.7.2, 4.7.3, and 4.7.4 shall be applied during ESAD development.

4.7.1 Electromagnetic radiation (EMR)

ESADs shall not arm or function due to Electromagnetic Radiation (EMR) in any logistic and tactical configuration until launch and safe separation have been achieved. Electromagnetic emission sensitivity, susceptibility, or vulnerability of the ESAD shall not create a potential hazard. The requirements of MIL-STD-461 and DOD-STD-1463 shall apply. The general requirements and test methods to preclude hazards resulting from ordnance having electro-explosive devices are provided in MIL-STD-1385.

4.7.2 Electrostatic Discharge (ESD)

ESADs shall not arm or function due to Electrostatic Discharge (ESD). Requirements and test methods for ESD testing are given in MIL-STD-331.

4.7.3 Electromagnetic pulse (EMP)

ESADs shall not function due to Electromagnetic Pulse (EMP). The EMP test environment is specified in DOD-STD-2169.

4.7.4 Lightning effects

ESADs shall not arm or function due to the effects of lightning. Requirements for lighting testing and evaluation shall be in accordance with MIL-STD-1795 and MIL-STD-1757.

4.7.5 Power Supply Transients

ESAD circuits shall be designed to withstand any credible power supply voltage transients in either direction.

4.8 Reviewing authority

All new or altered designs, or new applications of approved designs, shall be presented for a safety evaluation and certification of compliance or appropriate waiver considerations to:

Chairman,
Weapon System Explosives Safety Review Board
Naval Sea Systems Command
Washington, DC 20362

5. DETAILED REQUIREMENTS

5.1 General

The safety criteria contained herein should be selectively applied in accordance with the needs of specific ESAD development programs.

5.2 Explosive trains

5.2.1 Maximum acceptable safe stimulus (MASS) determination

The Maximum Acceptable Safe Stimulus (MASS) (see definition 3.1.24) shall be determined by analysis and testing. Testing of the initiator at the presumed MASS shall establish that the initiators shall not degrade or initiate with a reliability of .995 with confidence of 95%.

5.2.2 Explosive sensitivity (lead and booster explosives)

Explosives listed in Table I of MIL-STD-1316 are approved by all services for use in a position leading to the initiation of a high explosive main charge without interruption. Changes to this table may only be made by the procedures described in MIL-STD-1316. Explosives not listed in Table I must be approved by the associated safety authority board and an appropriate test plan developed to verify their suitability. Additional explosives for application to Navy devices may be approved by separate correspondence. Approved explosives shall be requalified in the ESAD and certified by the associated safety authority board as acceptable for that ESAD. The explosive material used in ESADs shall not be altered by any means (grinding, precipitation, recrystallization, density changes, etc.) likely to increase its sensitivity beyond that at which the material was qualified and at which it is customarily used.

5.2.3 Explosive train interruption

When an element of the explosive train contains primary explosives, at least one interrupter (shutter, slider, rotor) shall separate them from the lead and booster explosives until the arming sequence is completed. The interrupter(s) shall be directly locked mechanically in the safe position by at least two independent safety features. The safety features shall not be removed until the arming sequence begins. If the primary explosive material is housed in the interrupter, a single interrupter locked by the two independent safety features is acceptable. If the primary explosive is positioned such that safety is completely dependent upon the presence of an interrupter, the design shall include positive means to prevent the fuze or initiating system from being assembled without the properly positioned interrupter. The effectiveness of the interruption shall be determined by techniques described in MIL-STD-331 during design evaluation.

5.2.4 Non-interrupted explosive train control

5.2.4.1 Function energy control. Explosive train interruption is not required when the explosive train contains only booster and lead explosive materials allowed by 5.2.2. One of the following methods of controlling function energy shall be employed to preclude arming before achieving the required arming delay:

a. For ESADs containing energy greater than the MASS prior to expiration of the arming delay, at least two independent energy interrupters, each controlled by an independent safety feature, shall prevent the flow of energy to the initiator until completion of the safe separation delay. Additionally, the fuze or initiating system shall not be capable of functioning in the absence of the energy interrupter(s). This requirement applies to all ESAD designs that contain energy sources capable of producing the MASS.

b. For systems using techniques for accumulating functioning energy from the post-launch environment, the ESAD shall not permit any energy to reach the initiator until verification, by the ESAD, of a proper launch and attainment of the required safe separation. Additionally, any energy of the type required to function the initiator which exists in the ESAD or is available from the weapon system prior to attainment of the required arming delay shall be less than the MASS. The combined probability of having the MASS in the ESAD, having a failure of the energy control feature(s) and firing the initiator with the MASS energy shall be compatible with the specified ESAD safety system failure rate (see 4.3).

5.2.4.2 Electrical Initiator Sensitivity. The initiator for an electrically fired non-interrupted explosive train:

a. Shall meet the characteristics listed for 1-watt/1-amp initiators of MIL-STD-1512
b. Shall not be capable of being initiated or degraded in an unsafe manner by any electrical potential of less than 500 volts
c. Shall not be initiated as a result of exposure of the ESAD to the effects of lightning and specified electromagnetic radiation (EMR), electrostatic discharge (ESD), electromagnetic pulse (EMP) and nuclear radiation environments. Lightning test and evaluation shall be according to DOD-STD-1795 and MIL-STD-1757. EMR requirements and evaluation shall be according to MIL-STD-461 and DOD-STD-1463. ESD tests and evaluations shall be in accordance with MIL-STD-331. EMP tests and evaluations shall be in accordance with DOD-STD-2169.

5.3 Design features

5.3.1 Sterilization/Disable/Self-destruct features

The design of the ESAD shall incorporate a planned, programmed process consistent with the particular weapon and its use that:

a. Renders the weapon permanently incapable of functioning after specified events and time when the weapon has served its useful purpose, and/or
b. Renders the weapon temporarily incapable of functioning (e.g., by command enable/disable during launch cycle and flight) before or after specified events that could endanger the launch platform or friendly forces, and/or
c. Destroys the weapon after specified events and time when the weapon has served its useful purpose.

Designs not incorporating sterilization features shall provide justification and receive concurrence from the service safety review authority.

5.3.1.1 Sterilization of torpedoes and sea mines. ESADs for torpedoes and sea mines shall provide for sterilization after safe jettison, after specified events and time when the munition has served its useful purpose or when the munition is no longer capable of functioning reliably.

5.3.2 Fail-safe design

ESADs shall incorporate fail-safe design features based on their applicability to system requirements.

6. NOTES

This section contains information of a general or explanatory nature that may be helpful, but is not mandatory.

6.1 Intended use

This document establishes specific design safety criteria for ESADs. The criterion herein must be tailored to the specific ESAD development.

6.2 Safety Review

All new or altered designs, or new applications of approved designs shall be presented to the review authority of 6.3 for a safety evaluation of compliance with MIL-STD-1316 and this document. Included for presentation shall be documentation that details the design's safety attributes.

6.3 Custodian of Navy approvals for in-line lead and booster explosives and fuze and S&A designs.

Chairman
Weapon System Explosives Safety Review Board
Naval Sea Systems Command
Washington, DC 20362

6.4 Subject term (key word) listing

Delay, arming
Explosive ordnance disposal
Explosive train
Explosive train interruption
Fail-safe
Function, early
Function, premature
Fuze
Fuze design, safety criteria for
Safe and Arm Device
Electronic Safe and Arm Devices

Appendix A

Guidelines for the Application of the ESAD Technical Manual

A.1 Guidelines

The following guidelines are offered to assist the user in the interpretation of the requirements of the WSESRB Technical Manual. These guidelines attempt to describe the intent behind specific requirements where they are subject to interpretation. Guidelines are referenced by applicable paragraph numbers.

A.1.1 Purpose

A.1.2 Scope of Applicability

The application of this technical manual to ESADs transported by the Navy for other services, etc. extends only to those requirements applicable to the storage and transportation of the items. Therefore, specific criteria that apply to the safety of the item during operational use may not be applicable for non-Navy munitions. The application of this manual to U.S. Marine Corps developed or deployed items shall be to the extent specified by the Commandant, Marine Corps.

A.1.3 Excluded Munitions

This document applies to all munitions using electronic safety and arming devices except those used to initiate Nuclear warheads. It does, however, apply to ESADs used to enable other functions (e.g., rocket motors) for nuclear weapons.

A.3. DEFINITIONS

A.3.1 General

A.3.1.1 Arm

The arm definition is intended to provide a distinction between safe to handle state and an unsafe to handle state. This definition does not consider a reliable armed condition.

A.3.1.2 Arm-Fire Devices
A.3.1.3 Arming delay
A.3.1.4 Assembled fuze or initiating system
A.3.1.5 Booster and lead explosives
A.3.1.6 Credible environments
A.3.1.7 Dud
A.3.1.8 Dynamic electrical safety feature
A.3.1.9 Early-function
A.3.1.10 Electronic Safety and Arming Devices
A.3.1.11 Enabling

A.3.1.12 Environment
A.3.1.13 Environmental stimulus
A.3.1.14 Explosive Ordnance Disposal
A.3.1.15 Explosive train
A.3.1.16 Fail-safe design
A.3.1.17 Firmware

Firmware is software and must be developed, analyzed and tested in accordance with accepted software engineering methodologies and practices such as those defined in DOD-STD-2167A. Firmware shall be subjected to quality assurance provisions in the same manner as software.

A.3.1.18 Function
A.3.1.19 Fuze or Initiating System
A.3.1.20 Fuze or initiating system installation
A.3.1.21 Hand Grenades
A.3.1.22 Handheld Ordnance Devices
A.3.1.23 Independent safety feature
A.3.1.24 Initiator
A.3.1.25 Interrupted explosive train
A.3.1.26 Launch cycle
A.3.1.27 Main charge
A.3.1.28 Manual arming feature
A.3.1.29 Manually Emplaced Ordnance Items
A.3.1.30 Maximum Allowable Safe Stimulus
A.3.1.32 Mechanical safety feature
A.3.1.32 Neutralization
A.3.1.33 Non-interrupted explosive train
A.3.1.34 Premature function
A.3.1.35 Primary explosives
A.3.1.36 Pyrotechnic train
A.3.1.37 Safe Condition
A.3.1.38 Safe separation distance
A.3.1.39 Safety and Arming Device
A.3.1.40 Safety feature
A.3.1.41 Safety Interlock
A.3.1.42 Safety system
A.3.1.43 Safety system failure
A.3.1.44 Sensor, environmental
A.3.1.45 Sterilization

A.4. GENERAL REQUIREMENTS

A.4.1 General

A.4.1.1 Compatibility

A.4.2 ESAD Safety Systems

A.4.2.1 Safety redundancy

A.4.2.1.1 Enabling environments

"At least one sensed environment shall be verified continuously until munition safe separation is assured unless no practical environment is available." The intent of this requirement is to provide positive assurance that safe separation is achieved before full arming occurs. This specific requirement may not be possible in every situation (see tailoring guidelines in appendicies B through E). This requirement does not necessarily apply to ordnance not intended for use by the Navy or USMC.

A.4.2.1.2 Dynamic electrical safety feature(s)

The dynamic safety feature is intended to provide a fail safe design for at least one of the safety features. The requirement that the enabling environment be sensed continuously until safe separation is achieved will ensure that this safety feature, by itself, can provide an acceptable level of risk even in the presence of other failures.

A.4.2.1.3 Launch environments

A.4.2.1.4 Physical partitioning

"Functionally dissimilar elements" is intended to mean that the designs of the circuits should be substantially different in the way in which they function to reduce the probability of common mode failures. Examples include analog vs. digital design (e.g. timers) or microprocessor vs. discrete component designs. Digital circuits and microprocessors are somewhat more susceptable to EMI and ESD which could induce common mode failures. Another intent is to preclude having the elements of the same circuit controlling two safety features. This increases the risk of a single point failure affecting both features. Each circuit should control a safety feature (or outputs from both may control both features). Acceptable designs would include those that partition the circuits controlling the arming interruption into two physically dissimilar elements, provided that physically dissimilar is not interpreted as being minor design or fabrication differences.

"System arming shall not occur if any system electrical power sources, electrical grounds, or system frequencies are connected or disconnected in a credible manner to any point in the circuit." This requirement is intended to require the designer to demonstrate that the ESAD safety system cannot be compromised by a simple short of a ground, power, or normally occurring frequency source to any point in the circuit. Therefore, if a dynamic safety feature is driven at a certain frequency, the designer must ensure that the specific frequency is not present anywhere in the system (whether part of the ESAD or any closely related component) or that it is impossible for that frequency to compromise the ESAD arming system. Note that frequency harmonics must be addressed (e.g., a 12kHz oscillator in the circuit may provide a 36kHz signal possibly causing compromise of a dynamic safety feature intended

to operate at 36kHz) and frequencies derived from the environment (e.g., munition spin rate).

A.4.2.1.5 Manual Arming Features

"The design of the ESAD shall meet the system safety failure rate after [the manual] arming feature has been compromised...unless it can be shown by analysis and test that the feature will not be compromised by any credible life cycle environment." The probability of occurrence of compromise of the manual arming feature should be shown to be acceptable to the cognizant reviewing authority. For munitions transported by the Navy, the credible life cycle environment shall address those evolutions of transportation, handling and stowage by the Navy. Intentional or deliberate compromise of the feature by personnel is not considered to be within the scope of this requirement.

A.4.2.1.6 Safety feature type combinations

Item A in table 1 can represent either an interrupted explosive train design that complies with MIL-STD-1316 or a design that provides mechanical safety features on an electrical circuit that complies with the intent of MIL-STD-1316. Note that switches, relays, and similar devices that can interrupt the flow of electrical energy are considered static (generally) electrical features, not mechanical safety features.

A.4.2.1.7 Safety Interlocks

The safety interlock may be as simple as a monitor that prevents completion of the arming sequence in the event of an incorrect sequence of environments or timing problem, or a design that requires the environments to occur sequentially. Designs will be evaluated on an individual basis.

A.4.2.2 Arming delay

A.4.2.2.1 Safe Separation Safety

Safe separation requirements should be specified in the system design documents. Acceptable levels of risk to the launching platform and personnel must also be documented in the system design requirements. The design of the ESAD shall provide for a safe separation that meets the requirements and intent of the system design specification. Systems for which an acceptable level of risk has not been identified are subject to having a determination made by the service safety authority.

A.4.2.2.2 Timers

Early time out of a timer can be prevented in several ways. Redundant timers is one method that can be applied, however, the timers shall be designed to preclude common mode or single point failures. Alternate methods include using analog bandpass filters or tuned circuits on a timer output that will permit only frequencies within a specified range to pass. Tuning voltage conversion circuits in another method that may

be employed. Note that the requirement for physical partitioning would apply to any design involving redundant timers.

A.4.2.2.3 Post-safe separation safety

The requirements for and acceptable risk for post safe separation safety should be clearly specified in the system design documents. Systems will be evaluated on an individual basis.

A.4.2.3 Manual arming

A.4.2.4 Logic functions

A.4.2.5 Firmware

A.4.2.6 Application Specific Integrated Circuits

A.4.2.6.1 ASIC Design

"ASICs shall not incorporate unnecessary gates or functions in the design." This requirement is intended to apply to circuit functions that are not necessary to the operation of the ASIC in the application, or the testing and verification of ASIC operation during final acceptance, burn-in, or after installation. Note that programmable logic arrays are not automatically excluded from use by this requirement. Excess transistors not utilized by the ASIC design are not considered unnecessary gates or functions unless they have been inter-connected into a functional circuit.

A.4.2.6.2 ASIC Testing

A.4.3 Safety system failure rate

A.4.3.1 Analyses

Software Safety: Software that directly influences the enabling of an energy interruptor includes any signal generated by a microprocessor or other controller that can cause or allow the early or premature enabling of that energy interruptor. In other words, if a safety interlock is included in the software that monitors the arming sequence and causes an interruption in the event of an out-of sequence event, that software must be considered safety critical and subject to the appropriate analysis and testing. If the software is an additional control on the energy interruptor and cannot cause or allow a early or premature arming or enabling of the interlock, it is not safety critical and does not require the same degree of analysis and test. If software is used to provide for post-safe separation safety, the software must be factored into the overall risk assessment for this operational mode.

A.4.4 Design for quality control

Subparagraph c:
"Software development shall be done in accordance with accepted high quality software development procedures, such as DOD-STD-2167A."

Specific interpretation of what constitutes high quality software development procedures should be open to interpretation by the service safety reviewing authority.

A.4.5 Design approval

The cognizant safety authority has responsibility for the review and approval of ESAD designs during various stages of development. Their interpretation of the design criteria shall establish the precedent.

A.4.6 Design features

A.4.6.1 Stored energy

Stored energy sources shall not be used in ESADs unless there are no practical environmentally derived energy sources. An ESAD is considered to have stored energy if it is capable of accumulating a firing stimulus equal to or greater than the MASS. Capacitors that are charged immediately prior to launch are considered stored energy. Batteries in any form are considered stored energy even if they are normally initiated after launch. ESADs that do not contain sufficient energy to generate the MASS or are designed such that a firing stimulus cannot be accumulated even in the presence of credible failures, and rely on environmentally derived energy sources to accumulate the firing stimulus are not considered to have stored energy.

A.4.6.1.1 Lithium Batteries

Certain lithium battery designs have been shown to pose potential hazards to personnel and equipment. Due to the nature of some of these hazards, the Navy has issued policies regarding the use of lithium batteries in NAVSEA Notice 9310. This Notice also establishes guidelines and requirements for the design and testing of lithium batteries. All devices containing lithium batteries, whether used aboard ship or carried aboard ship, must comply with NAVSEA Notice 9310.

A.4.6.2 Explosive ordnance disposal (EOD)

It is the intent of the WSESRB to have full involvement of the Explosive Ordnance Disposal community in the design and development of munitions, including their fuzing systems. Designs deemed unacceptable or high-risk by EOD shall be considered unacceptable by the WSESRB.

A.4.6.2.1 EOD Design Features

A.4.6.2.2 EOD reviewing authority

A.4.6.3 Safe condition

A.4.6.3.1 Safe condition assurance options

A.4.6.3.2 Visual indication

This paragraph is intended to allow the option of incorporating a visual indication of the safe-arm status of the ESAD.

A.4.6.4 Firing Stimulus Dissipation

The firing stimulus dissipation mechanism should not be subject to single point or common mode failures. In addition, the mechanism shall be implemented such that failure of the dynamic safety feature will allow the firing stimulus to dissipate within the specified time.

A.4.7 Electromagnetic and electrical hazards

A.4.7.1 Electromagnetic radiation (EMR)

The ESAD shall remain operable after exposure to the EMR (susceptability and vulnerability) test environments.

A.4.7.2 Electrostatic Discharge (ESD)

The intent of this requirement is to ensure that electrostatic discharge, whether during manufacture, assembly, testing, or handling does compromise the safety of the ESAD.

A.4.7.3 Electromagnetic pulse (EMP)

The intent of this requirement is to ensure that EMP effects cannot compromise the safety of the ESAD. The ESAD should also remain operable after exposure to this environment.

A.4.7.4 Lightning effects

The intent of this requirement is to ensure that lightning effects cannot compromise the safety of the ESAD.

A.4.7.5 Power Supply Transients

The intent of this requirement is to ensure that power supply transients, whether as a result of normal or abnormal operation, cannot compromise the safety of the ESAD. The ESAD should also remain operable even in the presence of normal transients.

A.4.8 Reviewing authority

A.5. DETAILED REQUIREMENTS

A.5.1 General

A.5.2 Explosive trains

A.5.2.1 Maximum acceptable safe stimulus (MASS)

A.5.2.2 Explosive sensitivity

A.5.2.3 Explosive train interruption

This paragraph is included in the document for completeness. If primary explosives are used, the explosive train must be physically interrupted.

A.5.2.4 Non-interrupted explosive train control

A.5.2.4.1 Function energy control

A.5.2.4.2 Electrical Initiator Sensitivity

A.5.3 Design features

A.5.3.1 Sterilization/Disable/Self-destruct

A.5.3.1.1 Sterilization of torpedoes

A.5.3.2 Fail-safe design

The dynamic safety feature should normally provide a fail-safe design for one safety feature. The safety interlock monitoring the arming sequence may provide for a fail-safe design in the event the other safety feature(s) fail statically.

A.6. NOTES

A.6.1 Intended use

Although this document is being developed for application to Navy employed systems, it will be used to evaluate multiple service weapon systems.

A.6.2 Safety Review

A.6.3 Custodian of Navy approvals

A.6.4 Subject term (key word) listing

Appendix B

Application of the Design Criteria to Arm-Fire Devices

B.1.0 To Be Determined

Appendix C

Application of the Design Criteria to Hand Emplaced Ordnance

C.1.0 To Be Determined

Appendix D

Application of the Design Criteria to Hand-Held Ordnance

D.1.0 To Be Determined

Appendix E

Application of the Design Criteria to Hand Grenades

E.1.0 To Be Determined